CrowdStrike Technology Partners

CROWDSTRIKE

Solution Brief

GOOGLE CLOUD AND CROWDSTRIKE FALCON

Achieve defense in depth with cloud-scale cybersecurity strategies

CHALLENGES

Organizations adopting cloud-native applications face an increasingly diverse and sophisticated threat landscape, and require deeper integration of cloud services and security solutions, with shared responsibility for securing and controlling the cloud estate. The rise of DevSecOps teams — combining IT operations and security functions into one — has been occurring in enterprises that are instrumenting cloud-native security controls and integrating them with existing IT infrastructure.

SOLUTION

The CrowdStrike Falcon® platform provides comprehensive visibility into endpoints — and the workloads, events and instance metadata that enable detection, response, proactive threat hunting and investigation — to ensure that nothing goes unseen in your hybrid environments. Google Cloud service integrations with the Falcon platform include:

- Chronicle, Google Cloud's security analytics platform for accelerated incident response and proactive threat hunting
- VirusTotal for enriched threat intelligence
- Security Command Center (SCC) for threat detection aggregation
- BeyondCorp Enterprise for Zero Trust posture assessment and access control
- Google Operating System Configuration Management for automated and scalable sensor deployment

These integrations between Google and CrowdStrike's cloud-scale platforms leverage powerful APIs and rich telemetry to help deliver multi-level cybersecurity defense and drive effective, efficient solutions to the market.

KEY BENEFITS

Discover unknown threats with the right context and actionable intelligence

Expedite and augment incident response, increasing efficiency and productivity

Improve efficiency, ease of use and speed of deployment — with virtually no performance impact

Gain security posture visibility and control with continuous Zero Trust checks across workloads, endpoints and identities

GOOGLE CLOUD AND CROWDSTRIKE FALCON

BUSINESS VALUE

- **Comprehensive visibility and control:** Gain visibility into Google Cloud workload events and compute instance metadata with aggregated data findings — and enable detection, response, proactive threat hunting and investigation — to ensure that nothing goes unseen in your cloud environments.
- **Accelerated threat investigation and remediation:** By correlating the Falcon platform's rich endpoint and workload telemetry with Chronicle and Security Command Center, security teams can prioritize violations and investigate alerts, anomalies and threats with improved contextual insight to proactively stop cyberattacks.
- **Proactive defense with enriched threat intelligence:** VirusTotal provides access to enriched security data coming in from over 70 security vendors to increase investigation accuracy, and reduces alert fatigue by profiling adversaries and focusing on TTP-based threat hunting — all leading to improved security posture.
- **Frictionless Zero Trust-led security posture:** The seamless integration of the Falcon platform with BeyondCorp Enterprise converges users and endpoint risk assessment to prohibit access from untrusted hosts and improve security posture.

KEY CAPABILITIES

- **Discover unknown threats with the right context and actionable intelligence:** Eliminate blind spots with automatic indicator of compromise (IOC) feeds derived from VirusTotal dynamic campaign monitoring. Instantly pivot to related infrastructure and identify IOCs to feed your network perimeter defenses and cloud services.
- **Proactive threat hunting:** Hunt for threats across live and historical endpoint and workload security telemetry at unprecedented speed, with shared IOCs across Chronicle and the Falcon platform, providing proactive security. Profile adversaries with VirusTotal, conduct proactive TTP-based hunts and automatically generate detection rules that can be deployed in your endpoint detection and response (EDR).
- **Increased visibility and control:** With Security Command Center integration, gain additional visibility and control over your environment with a unified management console that consolidates aggregate security findings to help improve the security posture of your organization.
- **Real-time notification and remediation:** Notify users to take action deep within the family of Google Cloud services to correct policy violations and address security threats, based on detections and alerts from the Falcon platform.
- **Continuous Zero Trust checks:** Automate ongoing Zero Trust assessments of all managed devices running Windows and macOS, sent through APIs to BeyondCorp Enterprise to prohibit access from untrusted hosts and improve security posture.

WHY CHOOSE FALCON CLOUD SECURITY

Automatically gain insight into the scope and nature of cloud workloads to mitigate attacks and reduce risk

Gain comprehensive visibility into workload and container events and compute instance metadata to eliminate blind spots

Protect against active attacks and threats when cloud workloads are the most vulnerable — at runtime

Simplify deployments with cloud services without custom scripts, leveraging rich API and data stream integrations

In addition to deep integrations, the CrowdStrike Falcon platform offers comprehensive visibility into cloud workload events and instance metadata and cloud security posture management solutions (CSPM). Falcon Cloud Workload Protection provides detection, investigation, response and proactive threat hunting capabilities across cloud workloads and containers. DevOps and DevSecOps teams can identify and correct any misconfigurations or vulnerabilities using CrowdStrike Falcon Horizon™ CSPM, which provides visibility across multiple environments and reduces alert fatigue for security operations centers.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.